COURSE SYLLABUS

LAST REVIEW	Fall 2022
COURSE TITLE	Information Assurance & Data Protection
COURSE NUMBER	CIST 0225
DIVISION	Career and Technical Education
DEPARTMENT	CIST
CIP CODE	24.0101
CREDIT HOURS	3
CONTACT HOURS/WEEK	Class: 3 Lab:
PREREQUISITES	CIST 0101

COURSE DESCRIPTION

This course will provide students with the required skills to implement and apply technical knowledge of security concepts. Students will gain a deep knowledge in systems access control, cryptography and systems security threads. The gained skills from this course are important for intrusion detection systems, physical access control and multi-factor and many other system security issues. Students will be given real world scenarios to reinforce the material covered in this course and they will learn how to apply the learned concepts to their daily operations.

PROGRAM ALIGNMENT

This course is part of a program aligned through the Kansas Board of Regents and Technical Education Authority. For more information, please visit: https://kansasregents.org/workforce_development/program-alignment

PROGRAM LEARNING OUTCOMES

1. Demonstrates the necessary skills to score at least a 70% in the Network 1 course.
2. Obtain the skills necessary to pass the Certification COMPTIA SEC+ certification.
3. Applies judicious and ethical offensive security techniques using knowledge gained through cyber security coursework.
4. Obtain the skills necessary to pass the NET+ certification.

TEXTBOOKS

http://kckccbookstore.com/

METHOD OF INSTRUCTION

A variety of instructional methods may be used depending on content area. These include but are not limited to lecture, multimedia, cooperative/collaborative learning, labs and demonstrations, projects and presentations, speeches, debates, panels, conferencing, performances, and learning experiences outside the classroom. Methodology will be selected to best meet student needs.

COURSE OUTLINE

I. Threats and Vulnerabilities
   A. Types of malware.
   B. Various types of attacks.
   C. Social engineering attacks and the associated effectiveness with each attack.
   D. Wireless attacks.
   E. Application attacks.
   F. Mitigation and deterrent techniques.
   G. Tools and techniques to discover security threats and vulnerabilities.
   H. Penetration testing and vulnerability scanning.

II. Access Control and Identity Management
   A. Function and purpose of authentication services.
   B. Authentication, Authorization and Access control (AAA).
   C. Install and configure security controls for account management.

III. Cryptography
   A. Cryptography concepts.
   B. Cryptographic methods.
   C. Public Key Infrastructure (PKI), Certificate management and associated components.

COURSE LEARNING OUTCOMES AND COMPETENCIES

Upon completion of the course, the student will:

A. Define types of malware.
   1. Define Adware, Virus, Spyware Trojan, Rootkits & Backdoors.
   2. Define Logic bomb, Botnets Ransomware, Polymorphic malware & armored virus.
   3. Define DDoS, Smurf attack, Spoofing, Spam, Phishing, Spim & Vishing
   4. Define Spear phishing, Xmas attack, Pharming, Privilege escalation & Malicious insider threat.
   5. Define DNS poisoning and ARP poisoning, Transitive access, Client-side attacks, Typo squatting/URL hijacking & Watering hole attack.
   6. Define Password attacks: Brute force, Dictionary attacks, Hybrid, Birthday attacks & Rainbow tables.

B. Explain social engineering attacks

7. Explain the principles social engineering attacks.
8. Explain Shoulder surfing, Dumpster diving & Tailgating.
9. Explain Impersonation, Hoaxes, Whaling & Vishing.

C. Explain wireless attacks

10. Explain Rogue access points, Jamming/interference & Evil twin.
11. Explain War driving, Bluejacking, Bluesnarfing & War chalking.
12. Explain IV attack, Packet sniffing & near field communication.
13. Explain Replay attacks, WEP/WPA attacks& WPS attacks.

D. Explain application attacks.

14. Explain Cross-site scripting, SQL, LDAP & XML & Directory traversal/command injection.
15. Explain Buffer & Integer overflow, Zero-day, Cookies and attachments & Locally Shared Objects.
16. Explain Flash cookies, malicious add-ons, Session hijacking, Header manipulation & arbitrary code execution/remote code execution.
17. Explain Monitoring system logs: Event logs, Audit logs, Security logs & Access logs.
18. Explain Disabling unnecessary services & accounts, Protecting management interfaces and applications & Password protection.
19. Explain MAC limiting and filtering, 802.1x, disabling unused interfaces and unused application service ports & Rogue machine detection.
20. Explain Security posture: Initial baseline configuration, Continuous security monitoring & Remediation.
21. Explain Reporting (Alarms, Alerts & Trends) & Detection controls vs. prevention controls.

E. Explain tools and techniques to discover security threats and vulnerabilities.

22. Explain Interpret results of security assessment tools: Protocol analyzer, Vulnerability scanner, Honeypots, Honeynets, Port scanner, Passive vs. active tools & Banner grabbing.
23. Explain Risk calculations (Threat vs. likelihood), Assessment types (Risk, Threat & Vulnerability) & Assessment technique (Baseline reporting, Code review, Determine attack surface, Review architecture & designs).
24. Explain Penetration testing: Verify a threat exists, Bypass security controls, actively test security controls & Exploiting vulnerabilities.
25. Explain Vulnerability scanning: Passively testing security controls, Identify vulnerability, lack of security controls & common misconfigurations, Intrusive vs. non-intrusive scanning, Credentialed vs. non-credentialed scanning & false positive.
26. Explain Black, White & Gray box.

F. Explain authentication services

27. Explain RADIUS, TACACS+, Kerberos, LDAP, XTACACS, SAML & Secure LDAP.

G. Explain the concepts of AAA

28. Define Authorization: Least privilege, Separation of duties, ACLs, Mandatory access, Discretionary access, Rule & Role-based access control & Time of day restrictions.
29. Define Authentication: Tokens, Common access card, Smart card, Multifactor authentication, TOTP, HOTP, CHAP, PAP, Single sign-on, Access control, Implicit deny & Trusted OS.
30. Explain Authentication factors: Something (you are, you have, you know), somewhere you are & something you do.
31. Explain Identification (Biometrics, Personal identification verification card & Username).
32. Explain Federation & Transitive trust/authentication.

H. Install and configure security controls for account management

33. Mitigate issues associated with users, multiple account, roles and/or shared accounts.
34. Define Account policy enforcement: Credential management, Group policy, Password complexity, Expiration, Recovery, Disablement, Lockout, Password history, reuse & length & Generic account prohibition.
35. Explain Group-based privileges, User-assigned privileges, User access reviews & Continuous monitoring.

I. Explain cryptography concepts

36. Explain Symmetric vs. asymmetric, Session keys, In-band vs. out-of-band key exchange & encryption methods (Block vs. stream).
37. Explain Transport encryption, Non-repudiation, Hashing, Key escrow, Steganography, Digital signatures, Elliptic curve and quantum cryptography, Ephemeral key & perfect forward secrecy.

J. Define cryptographic methods

38. Explain Comparative strengths and performance of algorithms.
39. Explain Use of algorithms/protocols with transport encryption (SSL, TLS, IPSec, SSH & HTTPS).
40. Explain Cipher suites & Key stretching: (PBKDF2 & Bcrypt).
41. Explain Certificate authorities and digital certificates (CA, CRLs, OCSP & CSR).
42. Explain PKI, Recovery agent, Public & Private key, Registration, Key escrow & Trust models.

ASSESSMENT OF COURSE LEARNING OUTCOMES AND COMPETENCIES

Student progress is evaluated through both formative and summative assessment methods. Specific details may be found in the instructor's course information document.

COLLEGE POLICIES AND PROCEDURES

Student Handbook
https://www.kckcc.edu/files/docs/student-resources/student-handbook-and-code-of-conduct.pdf

College Catalog
https://www.kckcc.edu/academics/catalog/index.html

College Policies and Statements
https://www.kckcc.edu/about/policies-statements/index.html

Accessibility and Accommodations
https://www.kckcc.edu/academics/resources/student-accessibility-support-services/index.html.